RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: SBV-T02

Lessons from a Founding Application Security Engineer

Kalyani Pawar

Application Security @ Zipline
Security Nerd
X: @AppsecRani

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Opinions are my own, and DO NOT represent my Employer

$whoami

- Hi! I am **Kalyani Pawar**
- I also go by **Kaylee**
- Application Security Expert, **Zipline**
- **Speaker** and **Reviewer** at Major Conferences
- Cohost, **Application Security Weekly**
- **Expertise:** Startup Security Posture, LLM Security, Leveraging AI for Security

APPSEC VILLAGE

women in CYBERSECURITY WiCyS

Application Security Weekly

BSIDES

What are we going to talk about today

- Why Startup Security Feels Different
- Avoiding the “Dump-and-Run” Security Approach
- Embedding Security into Engineering Culture
- Role-Based Takeaways: Founders, Devs, First Sec Hire
- Leveraging AI Prompts to Design Your Security Program

Startup security: Why does it even matter?

- **60%** of small businesses, including startups, close within 6 months of a breach (Source: Cybersecurity Ventures)
- **$120K–$1.24M** average cost for small orgs to respond to a data breach (Source:PurpleSec)
- **AI-powered malware** like GhostGPT is bypassing filters (Source: Mimecast, 2024)

“They just didn’t see it coming”

The Illusion of Velocity Trap

Before: Yass let's ship fast! 🏎️🏎️🏎️ (... and compromise on security 👀)"

After: "Last Friday, our service was exposed on the public internet…"

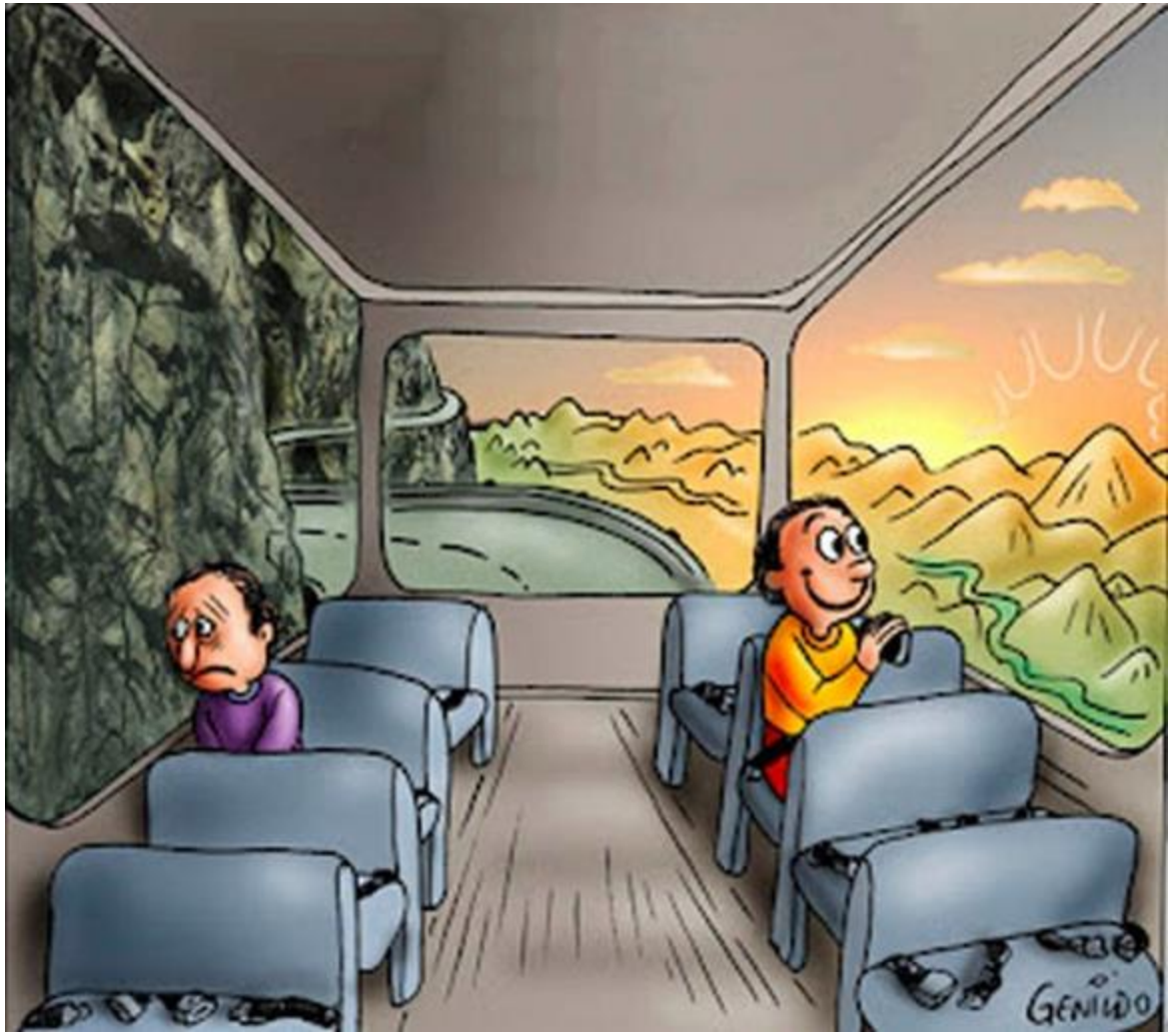
- Security Debt == Tech Debt
- Failed Vendor Security Reviews → Last Minute Scramble
- Missed Security → Loss in Sales

Lets flip the Security Mindset!

"Security slows us down..."

"Security is a compliance checkbox"

"Security is the security team's job."



"Good security prevents future slowdowns."

"Good security gets enterprise deals, earns customer trust."

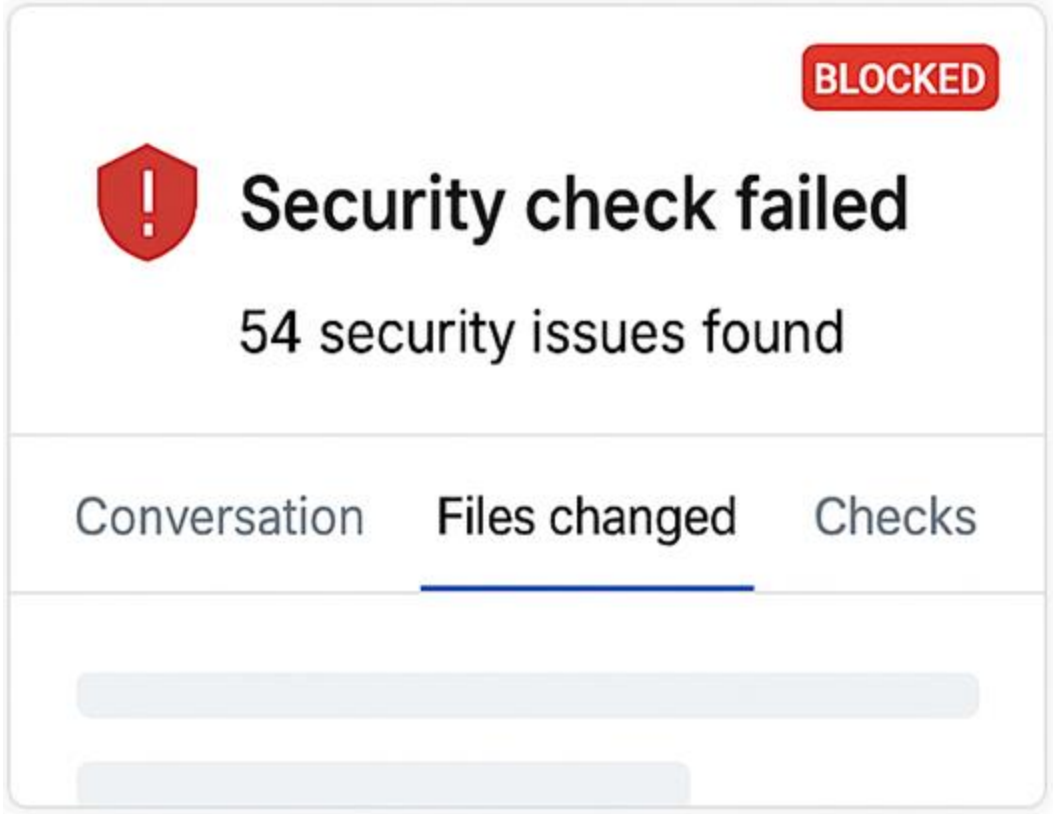
"Security is everyone's job."

Avoiding the prescriptive approach

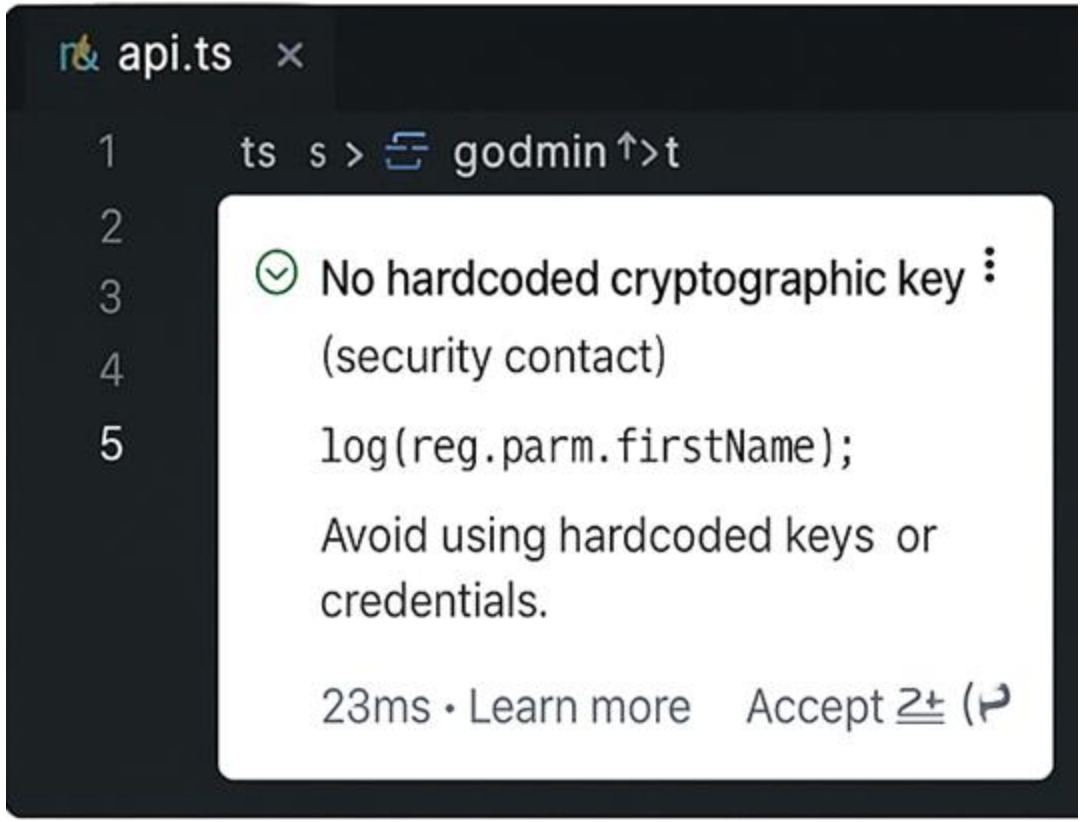
Avoiding the prescriptive approach

Security that understands your product >>> Security that checks boxes.

Build Paved Roads, Not Roadblocks



Traditional Security

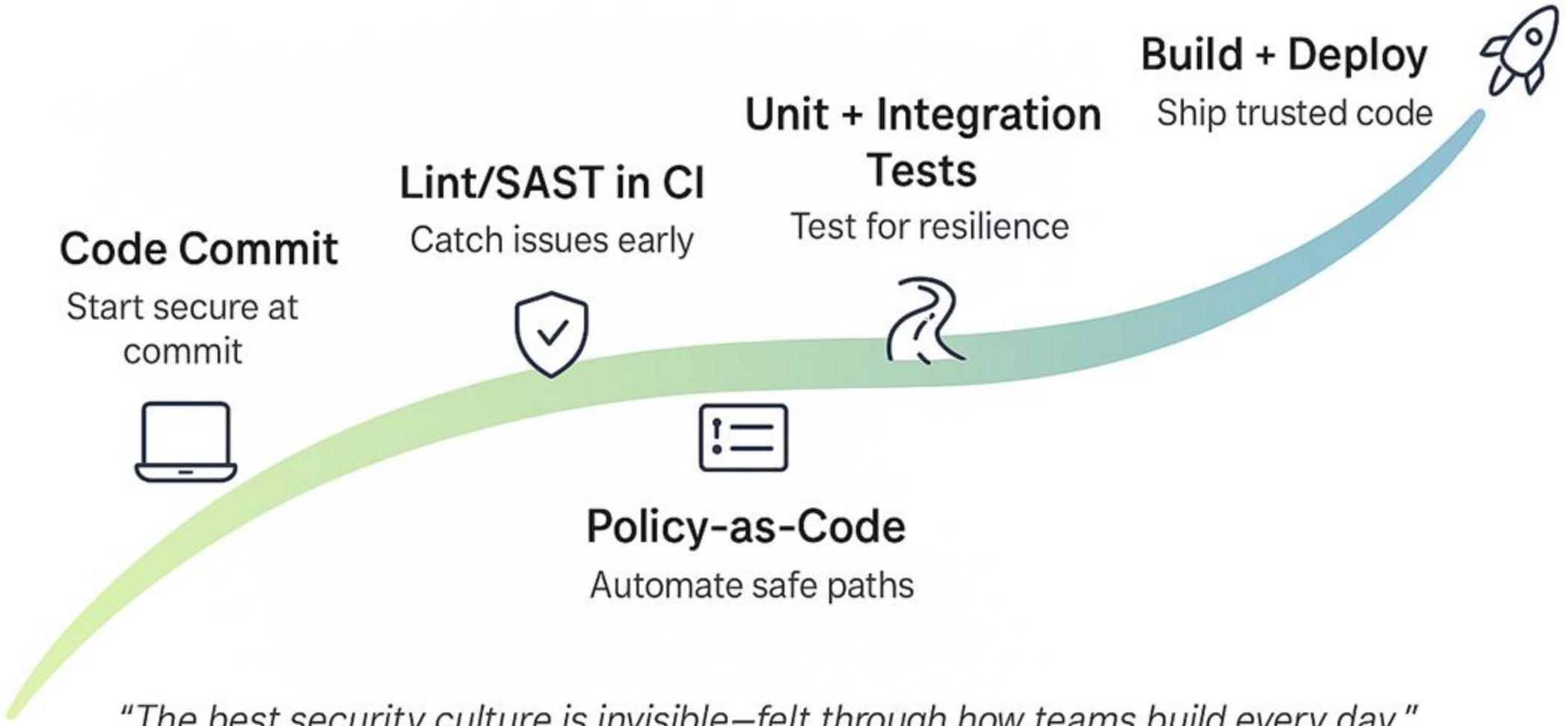


“Baked-in” Security

What is “Culture”?

“Culture is how your company makes decisions when you’re not there.”

Culture as Code



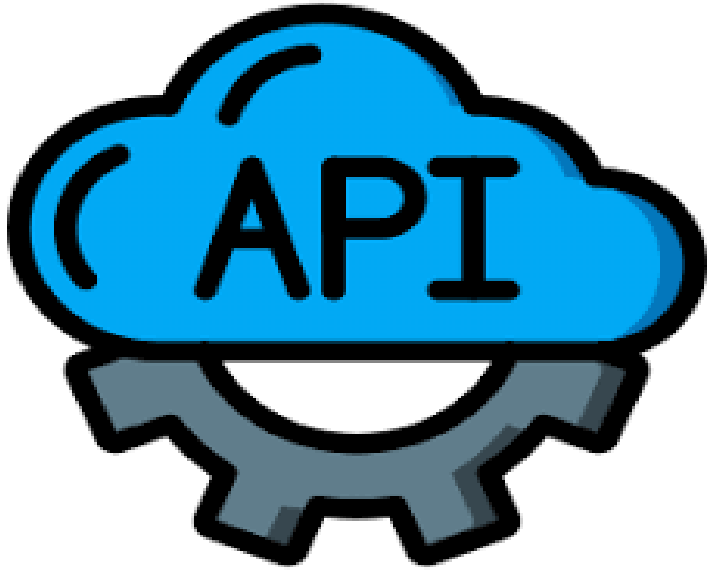
"The best security culture is invisible—felt through how teams build every day."

Real World Case Studies

Mintlify (2024)

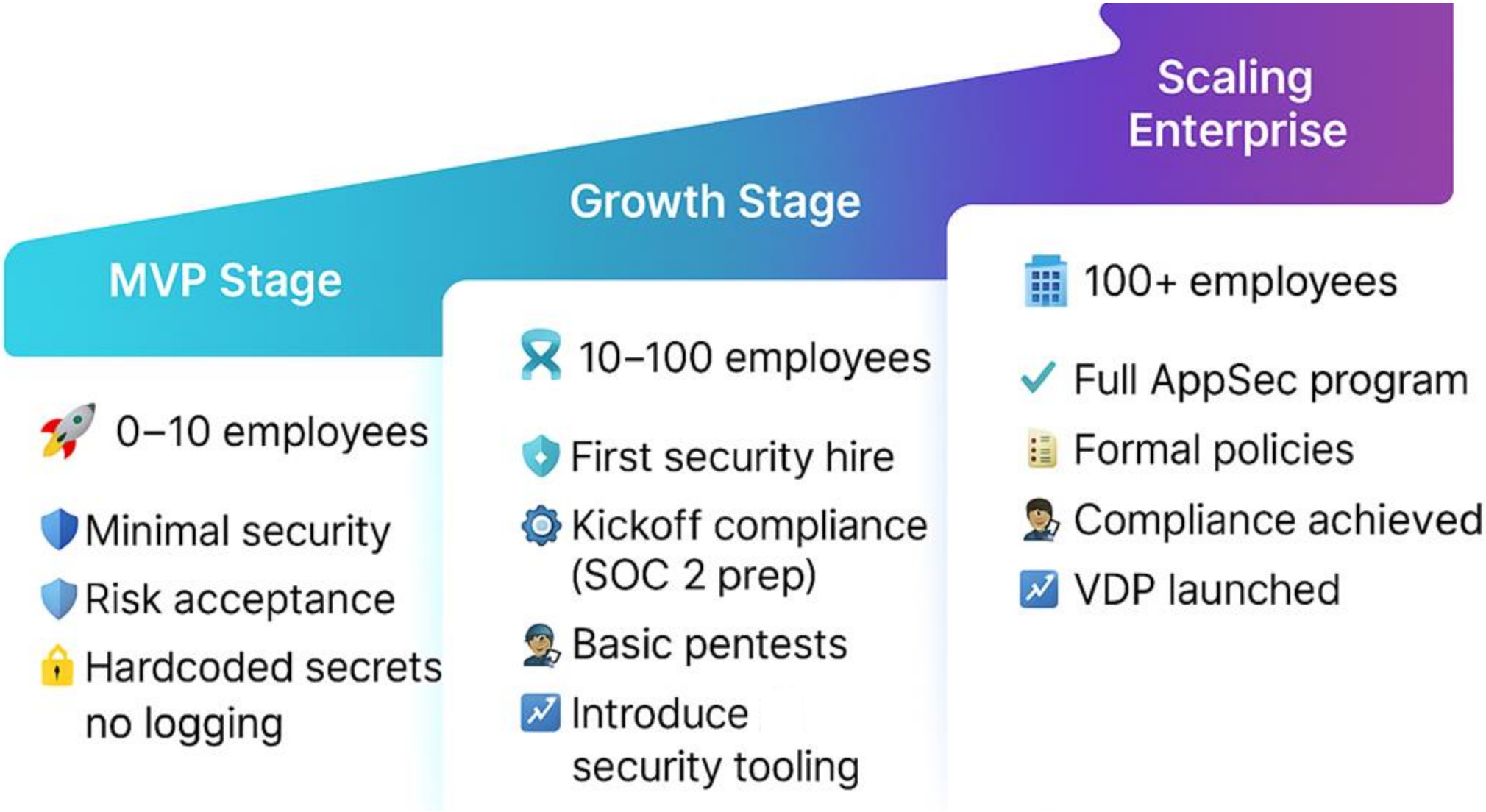
Weak Github Token Protection

PandaBuy (2024)



Critical API Auth Flaws

Security Maturity as You Scale



Security Growing Pains

Process

People

Tech Stack

Founder Specific Takeaways

“Users trust us with their data. That trust is valuable”

- Celebrate Security Wins Loudly
- Build a Security Conscious Culture
- Minimize PII Collection, Reduce Breach Risk
- Assign Clear Security Owners
- Get Legal Advice Often and Early
- Help Customers Use Your Product Securely

For Founding Engineers & Developers

“Security isn’t a feature; it’s a foundation.”

- ✅ Follow Secure Coding Standards
- 🔑 Secure Secrets and APIs Early
- 🛡️ Pentest the MVP — Catch Issues Fast
- 📚 Use Popular Frameworks with Built-in Security
- 🚫 Avoid Reinventing Security Libraries
- 🏗️ Involve Security Early in CI/CD

First Security Hire: Build + Automate Early Wins

“Good security is invisible. Bad security is obvious.”

Do This	Ask AI for Help *
Remove Admin Access	“Suggest least-privileged IAM policies for dev users”
Restrict Sensitive APIs	“Brainstorm API Gateway rules to enforce authN/authZ”
Prefer Temporary Keys	“Draft policy: Rotate keys every 24h”
Defense-in-Depth	“Ask LLM: Outline layers for my serverless app”
Vulnerability Disclosure Policy	“Ask LLM: Research VDPs from startups in <> industry”

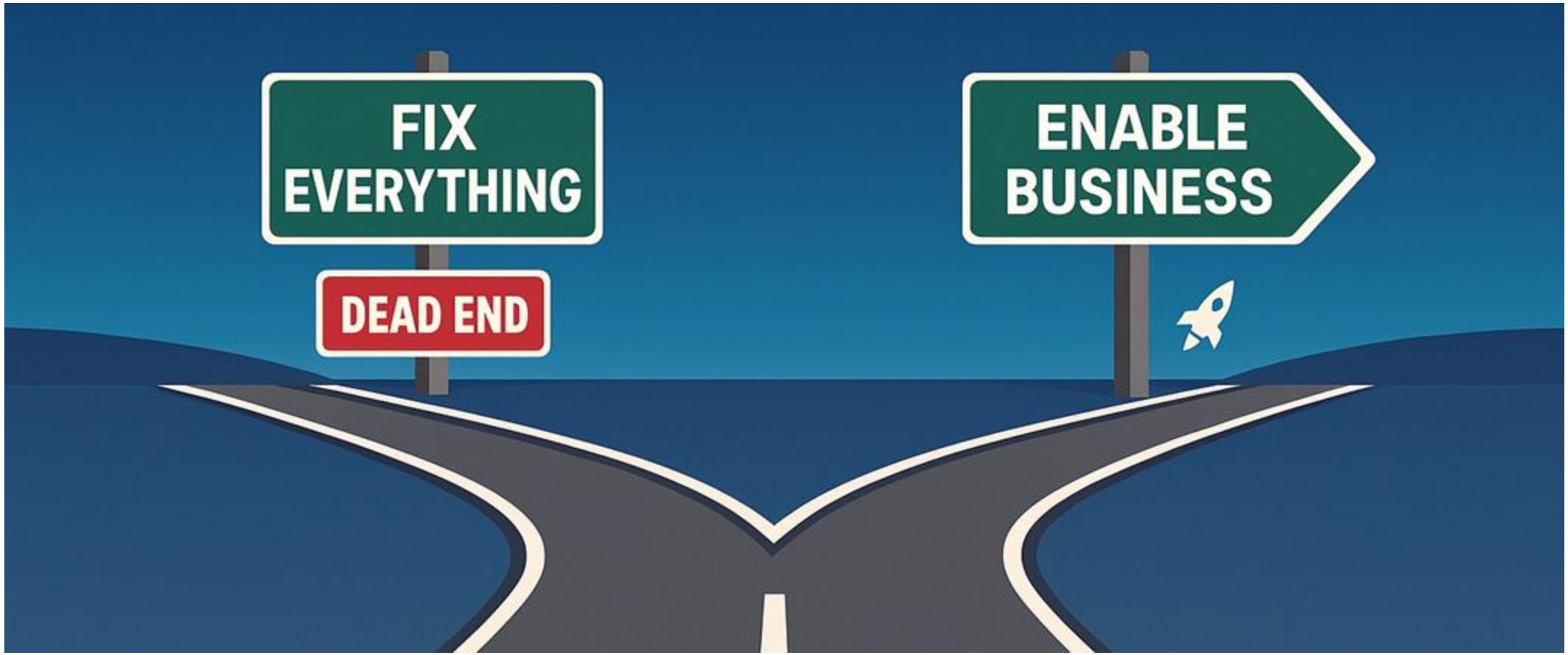
* Context matters. REALLY!

First Security Hire: What NOT to Do

- Running massive security trainings
- Dumping extensive problem lists on engineers
- Being the gatekeeper of security knowledge
- Skipping communication with stakeholders
- Running a public bug bounty immediately
- Neglecting preparation for Hiring

THE Lesson

“Your job isn’t to fix everything at once—it’s to make security a business enabler.”



Where Do We Go from Here?

- Do a little bit of every security thing
- Establish IR playbooks
- Document ALL the things
- Think in Systems, Not Just Tools
- Prioritize Risk Over Perfection
- Embrace the BUILDER function

“Apply” Slide - Next Week

- Identify **security ownership**
  - Even if there’s no dedicated hire, choose who is responsible for security
  - List out all the Low effort, High impact tasks
- Review **Public Exposure**
  - Audit S3, GitHub, APIs, endpoints
- Check for **hard coded secrets & API keys**
  - Run a scan, rotate credentials
- Enable basic logging & monitoring
  - If anything, at least log access to critical services/PII containing assets
- Do not underestimate **MFA**

“Apply” Slide - Within 3 Months

- Make sure to **Encrypt PII**
- Implement **Security Guardrails** in **CI/CD**
  - Enable SAST/SCA tooling
- Set up **centralized** logging & alerting
  - Define basic security alerts
- Start **tracking security debt**
  - Prioritize fixing high-risk security issues on the roadmap
  - Keep a “Security Debt” backlog in issue tracker
- Begin **compliance** prep (SOC 2, ISO 27001, GDPR if applicable)

“Apply” Slide - Within 6 Months

- Adopt **“Security as Code”** practices
- Secure third-party **dependencies & APIs**
  - Implement OAuth, API gateways, and rate limiting to prevent abuse.
- Implement a **lightweight incident response** plan
  - Define who handles security incidents (engineers, founders, legal)
  - Create an incident response checklist with clear escalation paths
- Build a **Vulnerability Disclosure Policy**
- Share **security wins & fails** internally and often

RSAC 2025 Conference

Many Voices.
One Community.

THANK YOU!

Use the QR Code to connect on LinkedIn!
X: @AppsecRani